SAP MIGRATION WITH F5

Confidently deploy your SAP apps in any cloud knowing that they're highly available, protected against malicious threats, and easily accessible to authorized users globally.

KEY CHALLENGES

Slow/Complex Migration

- Architectural complexity
- Greater operational strain
- Lack of standardization and control

SAP Application Security

- SAP vulnerabilities
- Advanced threats
- Regulatory compliance

Securing Access

- Enabling secure remote access
- Authorizing and simplifying access
- Ensuring consistent and simplified user experience

WHAT IS SAP FIORI AND S/4HANA?

As the mobile workforce took hold, the need for a more flexible, cross platform, and modern user experience was needed for SAP end users. Released in 2014, SAP Fiori was designed to deliver on this need, providing a web-based user experience that replaced the outdated SAP GUI for most functionality. With the 2.0 release, Fiori has become the de facto user experience for the majority of SAP enterprise applications including S/4, C/4, Ariba Mobile, and others.

Beneath Fiori lies the SAP Web Application Server, responsible for delivery of the end-user experience and content. Hosting the Java and ABAP services, users can now use any desktop or mobile browser for access.

ADVANCED APPLICATION LAYER SECURITY KEEPS SAP AVAILABLE AND PROTECTED

While SAP's modern application architecture empowers users, it also imposes the need for application-layer security to help mitigate sophisticated L7 threats and ensure availability to end users. These web-based application services expose a well-known and popular attack surface that needs to be protected from HTTP/S attacks and unauthorized users. As discussed in this SAP article, application layer firewalling is highly recommended to protect SAP deployments from web application attacks that traditional firewalls miss.

Augmenting that layer of perimeter security, an advanced authentication and authorization architecture ensures that unauthorized users and connections are blocked before they can connect to the SAP system. In addition to security, advanced traffic management is needed to provide SAP applications with high availability, reliability and performance.

Dynamic load distribution means that users are spread evenly across the best performing application servers and never sent to a server that is over capacity, behaving badly, or down. Overall system performance is increased when technologies like SSL offloading are leveraged. On the more advanced side of traffic management, SAP deployments can benefit from URL/URI based routing, allowing for seamless and transparent multi-tenancy.

F5 advanced application delivery and security services provide a highly effective way to secure, optimize, and direct traffic for SAP deployments.

KEY BENEFITS

- Streamlines migration through reusable policies and automated services
- Provides richness of choice across cloud providers, solutions and partners
- Complements SAP architecture with app security, global secure access and intelligent traffic management across hybrid environments

DEPLOYING THE F5 SOLUTION WITH SAP FIORI AND S/4HANA

F5 advanced application delivery and security services provide a highly effective way to secure, optimize, and manage application traffic and access for SAP deployments. F5 technology complements the SAP S/4HANA modern application architecture with a holistic perimeter-based security and advanced traffic management solution.

F5 technology modules make up the SAP migration solution and can run as separate instances or all on the same instance. They are offered on F5® BIG-IP® Virtual Edition (VE) virtual machines, running in private and public clouds or on the F5® BIG-IP® iSeries® or VIPRION® software-defined hardware appliances, running in the data center or colocation facilities. Hybrid deployments are also supported ensuring consistent application and security services across environments. F5 offers these solutions in packages to support a wide range of deployments from SME to very-large enterprise deployments.

The F5® BIG-IP® Local Traffic Manager™ (LTM), is the component providing load balancing, session state, SSL, and all other advanced traffic management needs.

The F5® BIG-IP® Advanced Firewall Manager™ (AFM) is a high-performance, stateful, full-proxy network security solution designed to guard data centers against incoming threats that enter the network while the F5® Advanced Web Application Firewall™ (Advanced WAF) provides the Layer 4-7 protection from the exposure of a web surface.

The F5® BIG-IP® Access Policy Manager® (APM) provides user security through the means of pre-authentication, single sign-on and federation.

The F5 SAP Migration Solution is available in a flexible package to suit any SAP deployment or migration to multi-cloud.

F5 TECHNOLOGY MODULES

F5 BIG-IP Local Traffic Manager (LTM)

F5 BIG-IP Advanced Firewall Manager (AFM)

F5 Advanced Web Application Firewall (WAF)

F5 BIG-IP Access Policy Manager (APM)

F5 SAP MIGRATION SOLUTION USE CASES

Quickly and Securely Migrate Your SAP Applications with F5 Solutions

STREAMLINE MIGRATIONS

F5 BIG-IP Platform

Lift and shift via existing policies and deployment guides with F5 iRules and Cloud Solution Templates. F5 offers a quicker way to migrate with tested and validated solutions through deployment guides, Cloud Solution Templates, and Automation Toolchain.

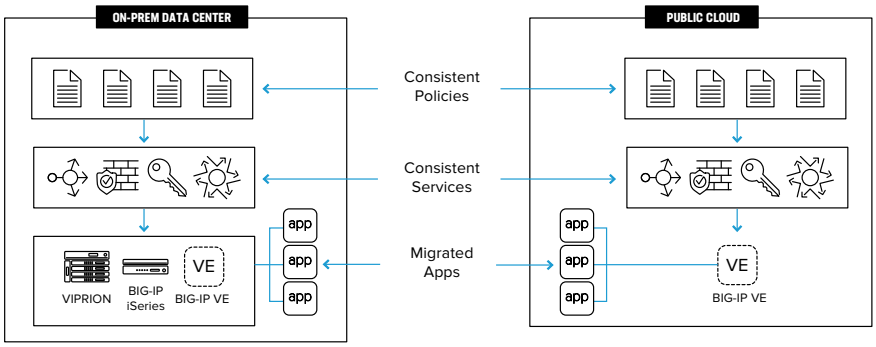

Figure 1: Streamline migration through reusable policies, automated services and intelligent traffic management across hybrid environments.

ADVANCED APP SECURITY

F5 Advanced WAF

Reduce risk while maintaining compliance and control with F5 Advanced WAF. Replicate on-premise security policies in the cloud, including consistent cross-environment visibility into app performance.

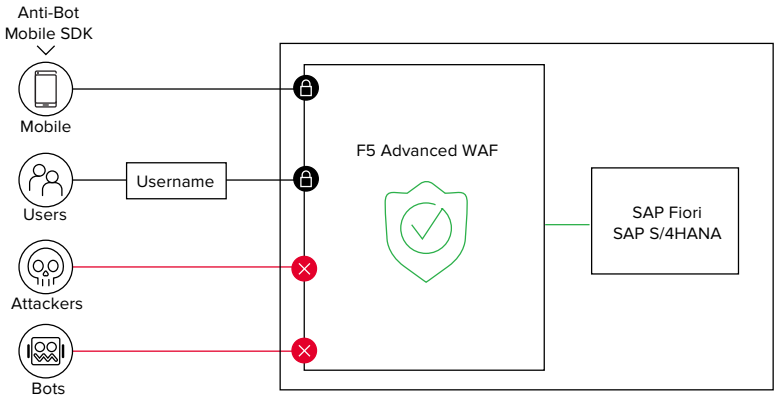

Figure 2: Protect your network against incoming threats, including the most massive and complex DDoS attacks.

SECURE IDENTITY AND ACCESS

F5 BIG-IP APM

Enforce access Policy and Identity Federation with single sign-on with multi-factor authentication. F5 helps you enforce access policies and identity federation for secure hybrid access to your SAP applications.

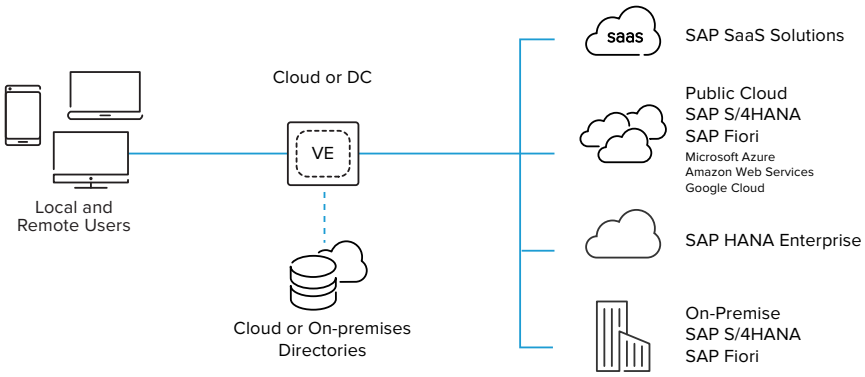

Figure 3: Unify application access across cloud providers, solutions and partners while enhancing security, usability, and scalability.

WHY F5 FOR SAP MIGRATION?

F5 technology provides an adaptable and agile multi-cloud application services architecture for SAP deployments. This allows organizations to ensure quality of service and manageability, apply business policies and rules to content delivery, support increasing traffic volumes, deliver applications securely, enjoy operational efficiency and cost control, and remain flexible to future application and infrastructure changes. The result is elegant and powerful solutions to protect you from security threats, network failures and traffic congestion, while providing an optimized architecture for the future.

To learn more, please contact us or visit SAP Migration with F5.